

# Referencia rápida consolidada acceso convergida para las plantillas del Wireless LAN

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Seguridad de la capa 2](#)

[ABRA la red inalámbrica \(WLAN\) ninguna Seguridad](#)

[Wired Equivalent Privacy \(WEP\) estático](#)

[Filtro MAC - Base de datos local](#)

[Filtro MAC - Radio externo](#)

[Clave previamente compartida protegida Tecnología inalámbrica del acceso 2 \(WPA2\) \(PSK\) autenticación local del Protocolo de Autenticación Extensible \(EAP\) del 802.1x \(NGWC usado como RADIUS local\)](#)

[802.1x en el radio externo](#)

[Seguridad de la capa 3](#)

[Passthrough de la red](#)

[Autenticación local de la autenticación Web](#)

[Autenticación Web con la autenticación de RADIUS externa \(ISE\)](#)

[Autenticación del Web externa](#)

[Autenticación Web personalizada con la autenticación local](#)

[Autenticación Web auto del ancla](#)

## Introducción

Este documento proporciona las plantillas de la configuración CLI de referencia rápida para las configuraciones básicas y sabidas del Wireless LAN de la capa 2 y de la capa 3 (red inalámbrica (WLAN)). Las plantillas bajas se proporcionan para una copia y una goma rápidas en el Wiring Closet de la última generación de Cisco las instalaciones iniciales del cliente (NGWC) 5760 y 3850 reconstrucciones del laboratorio del regulador del Wireless LAN (WLC) y.

## Prerequisites

## Requisitos

Cisco recomienda que usted tiene conocimiento la versión de 3.3 NGWC o de más adelante. Se

espera que las interfaces virtuales del Switch (SVI) y preconfiguran a los agrupamientos DHCP/snooping por las mejores prácticas.

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Seguridad de la capa 2

### ABRA la red inalámbrica (WLAN) ninguna Seguridad

```
wlan 1 name testwlan ssid testwlan
  client vlan 20
  no security wpa
  no shut
```

### Wired Equivalent Privacy (WEP) estático

```
wlan staticWEP 6 staticWEP
  client vlan 79
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security static-wep-key encryption 40 ascii 0 Cisco 1
  session-timeout 1800
  no shutdown
```

### Filtro MAC - Base de datos local

```
username 24770319eB75 mac

aaa new-model
aaa authorization network test_mac local

wlan macfiltering 6 macfiltering
  client vlan Vlan7
  mac-filtering test_mac
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  no shutdown
```

## Filtro MAC - Radio externo

```
aaa new-model
aaa group server radius wcm_rad

server name RAD_EXT
subscriber mac-filtering security-mode mac
mac-delimiter colon

radius server RAD_EXT
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key cisco

aaa authorization network wcm_macfilter group wcm_rad

wlan macfiltering 1 macfiltering
client vlan Vlan7
mac-filtering wcm_macfilter
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

## Clave previamente compartida protegida Tecnología inalámbrica del acceso 2 (WPA2) (PSK)

```
wlan wpa2psk 1 wpa2psk
client vlan 20
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 Cisco123
no shutdown
```

## autenticación local del Protocolo de Autenticación Extensible (EAP) del 802.1x (NGWC usado como RADIUS local)

```
user-name test
privilege 15
password 0 cisco
type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2 EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## 802.1x en el radio externo

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
 fast      EAP-FAST method allowed
 gtc      EAP-GTC method allowed
 leap     EAP-LEAP method allowed
 md5     EAP-MD5 method allowed
 mschapv2 EAP-MSCHAPV2 method allowed
 peap    EAP-PEAP method allowed
 tls     EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Seguridad de la capa 3

### Passthrough de la red

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
 fast      EAP-FAST method allowed
 gtc      EAP-GTC method allowed
 leap     EAP-LEAP method allowed
 md5     EAP-MD5 method allowed
```

```
mschapv2 EAP-MSCHAPV2 method allowed
peap     EAP-PEAP method allowed
tls      EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Autenticación local de la autenticación Web

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Autenticación Web con la autenticación de RADIUS externa (ISE)

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
```

```
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Autenticación del Web externa

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Autenticación Web personalizada con la autenticación local

```
ip http server
ip device tracking
```

```
aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local
```

```
username <username> password 0 <password>
```

FTP Configuration for file transfer:

```
ip ftp username <username>
ip ftp password <password>
```

Upload custom html files to flash: with command:  
5760# **copy ftp://x.x.x.x/webauth\_login.html flash:**

Example of flash content:

w-5760-2#**dir flash:**

Directory of flash:/

```
64649  -rw-          1164   Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654  -rw-          2047   Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655  -rw-          1208   Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656  -rw-           900   Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657  -rw-         96894   Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658  -rw-        23037   Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
64660  -rw-          2586   Oct 7 2013 13:31:27 +00:00  web_auth_aup.html
```

```
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
```

```
parameter-map type webauth custom
type webauth
redirect on-success http://www.cisco.com
banner text ^C CC global ip for redirect ^C
custom-page login device flash:webauth_login.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

```
wlan cisco 1 cisco
client vlan Vlanx
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list local_webauth
security web-auth parameter-map custom
session-timeout 1800
no shutdown
```

## Autenticación Web auto del ancla

```
//Verify//
```

```
show wireless mobility summary
```

```
<snip>
```

IP	Public IP	Group Name	Multicast IP	Link Status
192.168.100.8	-	ngwc	0.0.0.0	UP : UP
192.168.100.15	192.168.100.15	5760		UP : UP

```
radius server ise
address ipv4 192.168.154.119 auth-port 1812 acct-port 1813
key Cisco123
```

```
aaa group server radius rad_ise
server name ise
```

```
aaa authentication login ext_ise group rad_ise
parameter-map webauth global
virtual-ip ipv4 1.1.1.1
```

```
parameter-map type webauth test_web
    type webauth
    banner
```

WLAN configs on the Foreign 5760

```
wlan ngwc_guest 3 ngwc_guest
    client vlan 254
    mobility anchor 192.168.100.8 //Anchor
    no security wpa
    no security wpa akm dot1x
    no security wpa wpa2
    no security wpa wpa2 ciphers aes
    security web-auth
    security web-auth authentication-list wcm_local
    security web-auth parameter-map test_web
    no shutdown
```

WLAN configs on the Anchor 5760

```
wlan ngwc_guest 3 ngwc_guest
    client vlan 254
    mobility anchor 192.168.100.8 //Local
    no security wpa
    no security wpa akm dot1x
    no security wpa wpa2
    no security wpa wpa2 ciphers aes
    security web-auth
    security web-auth authentication-list rad_ise
    security web-auth parameter-map test_web
    no shutdown
```